James E. Cecchi
**CARELLA BYRNE CECCHI**
**OLSTEIN BRODY & AGNELLO, P.C.**
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700
*Interim Lead Counsel for Plaintiffs*
*(Additional Counsel on the Signature Page)*

**UNITED STATES DISTRICT COURT**
**DISTRICT OF NEW JERSEY**

| | |
|---|---|
| IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC. CUSTOMER DATA SECURITY BREACH LITIGATION<br><br>This Document Relates To: All Actions Against CareCentrix (Other Labs Track) | Civil Action No. 19-md-2904 (MCA)(MAH)<br><br>**CONSOLIDATED CLASS ACTION COMPLAINT: CARECENTRIX** |

**TABLE OF CONTENTS**

Plaintiffs, individually and on behalf of classes of all those similarly situated (the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to Plaintiffs and on information and belief as to all other matters, and upon the investigation conducted by Plaintiffs' counsel, bring this class action complaint against CareCentrix, Inc. ("CareCentrix"),[1] and allege as follows:

## PRELIMINARY STATEMENT

1. In June 2019, Defendant informed patients to whom it provided various healthcare services that an unauthorized user or users accessed the system run by CareCentrix's billing collections vendor, Retrieval-Masters Creditor's Bureau, Inc., d/b/a American Medical Collection Agency ("AMCA"), between August 2018 and March 2019 (the "Data Breach"). After accessing AMCA's systems, the hacker exfiltrated the sensitive personal, financial, and health testing information of millions of Defendant's patients and sold the information for profit on underground websites known as the "dark web."

2. Plaintiffs bring this class action because Defendant failed in its basic, legally bound, and expressly-promised obligation to secure and safeguard its patients' protected health information ("PHI") and personally identifiable information ("PII")—such as Plaintiffs' and Class Members' names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service and referring doctor) and other private information—such as credit and debit card numbers, bank account information, insurance, insurance subscriber identification number (all collectively referred to as "Personal Information").

[1] As additional facts come to light, Plaintiffs may respectfully seek leave to amend this Complaint in order to bring additional causes of action by plaintiffs from other states.

3. As of today, approximately 500,000 CareCentrix patients have had their Personal Information compromised as a result of the Data Breach. As a result of Defendant's failure to protect the consumer information it was entrusted—and legally obligated—to safeguard, Plaintiffs and Class Members suffered a loss of value of their Personal Information and have been exposed to and/or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. In fact, some Class Members' identities have already likely been stolen.

4. Defendant could have prevented this theft had it limited the customer information it shared with business associates and employed reasonable measures to assure its business associates implemented and maintained adequate data security measures and protocols in order to secure and protect customers' data.

5. Defendant's intentional, willful, reckless, and/or negligent conduct—failing to prevent the Data Breach, failing to limit its severity, failing to detect it in a timely fashion, and failing to timely notify Plaintiffs and the Class—damaged Plaintiffs uniformly. As discussed herein, fraudulent activities have already been linked to Defendant's conduct. For this reason, Defendant should pay for appropriate identity-theft protection services and reimburse Plaintiffs and the Class for the costs caused by Defendant's sub-standard security practices and failure to timely disclose the same. Plaintiffs and the Class are, therefore, also entitled to injunctive and other equitable relief that safeguards their information, requires Defendant to significantly improve its security, and provides independent, expert oversight of Defendant's security systems.

## JURISDICTION AND VENUE

6. This Consolidated Complaint is intended to serve as an administrative summary as to all other complaints consolidated in this multidistrict litigation asserting claims against

CareCentrix and shall serve for all purposes as an administrative device to aid efficiency and economy for the Class defined below. As set forth herein, this Court has general jurisdiction over Defendant and original jurisdiction over Plaintiffs' claims.

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 putative Class Members, and minimal diversity exists as Defendant and at least one Class Member are citizens different states.

8. This Court has personal jurisdiction over Defendant because it maintains sufficient minimum contacts in New Jersey such that it intentionally avails itself of this Court's jurisdiction by conducting operations here and contracts with companies in this District. Additionally, the United States Panel on Multidistrict Litigation transferred all related matters to this District, so Plaintiffs are bringing their claims against Defendant in this litigation before this Court.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the July 31, 2019 Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 2904 or, in the alternative, pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Defendant transacts business and may be found in this District.

## NAMED PLAINTIFFS

10. Plaintiffs are individuals who, upon information and belief, had their Personal Information compromised in the Data Breach, and bring this action on behalf of themselves and all those similarly situated both across the United States and within their State or Territory of residence. These allegations are made upon information and belief derived from, *inter alia*, counsel's investigation, public sources—including sworn statements, Defendant's website, and the

facts and circumstances currently known. Because Defendant has exclusive but incomplete knowledge of what information was compromised for each individual, including PHI, Plaintiffs reserve the right to supplement their allegations with additional facts and injuries as they are discovered.

11. Plaintiff Debbie Amico ("Amico") is a citizen and resident of the state of Florida.

12. Plaintiff Amico went to CareCentrix to obtain blood testing.

13. Plaintiff Amico provided CareCentrix with her Personal Information as part of obtaining blood testing.

14. On information and belief, Plaintiff Amico's bill from CareCentrix was subsequently sent to Defendant's billing-collections vendor, AMCA.

15. On July 10, 2019, Plaintiff Amico received a notice of the data breach at AMCA in connection with CareCentrix, stating that Plaintiff Amico's Personal Information may have been compromised.

16. As a CareCentrix patient, Plaintiff Amico believed that CareCentrix would protect her Personal Information, such as diagnostic information, once she provided it to CareCentrix or its vendors.

17. Plaintiff Amico would not have provided CareCentrix with this Personal Information nor used CareCentrix to provide blood testing had she known that it would fail to protect her Personal Information.

18. Plaintiff Amico suffered and will continue to suffer damages due to the Data Breach. Plaintiff Amico has spent substantial time to mitigate the adverse consequences of the Data Breach. To date, she has spent several hours trying to speak with AMCA or its representatives about the Data Breach, and she has spent at least one hour per week on monitoring

her credit and financial accounts for any unauthorized activity. Plaintiff Amico will have to spend considerable time going forward on monitoring for potential adverse consequences from the Data Breach, including, without limitation, credit card theft, identify theft, false-tax-return information submitted, a false loan submitted, expenses for credit monitoring, expenses for lifting credit-security freezes, and reduced credit scores.

19. Plaintiff L.D., minor by and through her mother and guardian Andrea Hall ("Hall"), is a citizen and resident of the state of Florida. Plaintiff L.D. makes all of the following allegations in this complaint by and through her mother and guardian, Hall, who is also a citizen and resident of the state of Florida.

20. Plaintiff L.D. went to CareCentrix to obtain medical services on or about June 1, 2017.

21. Plaintiff L.D. provided CareCentrix with her Personal Information as part of obtaining medical services.

22. The bill to Plaintiff L.D. from CareCentrix was subsequently sent to Defendant's billing-collections vendor, AMCA.

23. As part of billing-collections services provided for Defendant, Plaintiff L.D. has been contacted by AMCA through several letters, including on or around July 16, 2018 and August 27, 2018, and in response, Plaintiff L.D. (by and through her mother and guardian Hall) provided Personal Information to AMCA.

24. On July 10, 2019, Hall received a letter for Plaintiff L.D. regarding a notice of data breach involving AMCA in connection with CareCentrix, stating that Plaintiff L.D.'s Personal Information may have been compromised.

25. As a CareCentrix patient, Plaintiff L.D. believed that CareCentrix would protect her Personal Information once she provided it to CareCentrix or its vendors.

26. Plaintiff L.D. would not have provided CareCentrix with this Personal Information nor used CareCentrix to provide medical services had she known that it would fail to protect her Personal Information.

27. Plaintiff L.D. suffered and will continue to suffer damages due to the data breach. During 2018 and 2019, Hall received calls from a company fraudulently claiming to collect money for AMCA and asking for her credit card number. In September 2019, as a result of the data breach, Hall experienced at least one fraudulent charge for fast food of approximately $48 (that she did not pay) on her credit card, which was the same card used for expenses for Plaintiff L.D. (amongst other expenses), including being given to AMCA for CareCentrix bills. As a result of the data breach, Hall has changed her credit card information in response to fraudulent activity.

28. Hall has spent substantial time to mitigate the adverse consequences of the Data Breach. To date, she has spent several hours trying to speak with AMCA and CareCentrix representatives about the Data Breach and at least one hour per week monitoring credit and financial accounts for any unauthorized activity. Plaintiff L.D. will have to spend considerable time going forward on monitoring for potential adverse consequences from the Data Breach, including, without limitation, credit card theft, identify theft, false-tax-return information submitted, a false loan submitted, expenses for credit monitoring, expenses for lifting credit-security freezes, and reduced credit scores.

## DEFENDANT CARECENTRIX

29. Defendant CareCentrix is incorporated in the State of Delaware and is a health services management company with its headquarters at 20 Church Street in Hartford, Connecticut.

## FACTUAL ALLEGATIONS

### A. The Data Breach Impacted Patients Of A Wide Variety Of Laboratories, Including CareCentrix

30. Between August 1, 2018 and March 30, 2019, an unauthorized user or users gained access to the AMCA system that contained information obtained from various entities, including CareCentrix, as well as information that AMCA collected itself.

31. Approximately 500,000 CareCentrix patients have been affected by the Data Breach, making it one of the largest health-related data breaches reported to the U.S. Department of Health and Human Services ("HHS") in 2019.[2] The overall AMCA Data Breach (including all impacted laboratories) was the second largest to be reported since HHS's Office for Civil Rights launched its breach portal in 2010.[3]

32. On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark-web marketplaces where payment card data, and associated PII, is bought and sold. Almost 15% of these records of compromised payment cards included additional PII, such as dates of birth, Social Security numbers, and physical addresses. A thorough

---

[2] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Oct. 9, 2019); *see also August 2019 Healthcare Data Breach Report*, HIPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report/ (last visited Oct. 9, 2019).

[3] *July-reported healthcare breaches exposed 22 million people's data*, Modern Healthcare, https://www.modernhealthcare.com/cybersecurity/july-reported-healthcare-breaches-exposed-22-million-peoples-data (last visited Oct. 9, 2019).

analysis indicated that the information was likely stolen from the unsecure online portal of AMCA. Several financial institutions also collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[4]

33. "On March 1, 2019, Gemini Advisory attempted to notify AMCA," but as Gemini Advisory reportedly told DataBreaches.net, "they did not get any response to phone messages they left." Failing to obtain any response from AMCA, Gemini Advisory "promptly contacted federal law enforcement, which reportedly followed up by contacting AMCA."[5]

34. Following notification from law enforcement, AMCA's payment portal became unavailable for weeks.[6]

35. In a written statement attributed to AMCA in June, at the time, AMCA announced it was still investigating the breach:

> We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system," reads a written statement attributed to the AMCA. "Upon receiving information from a security compliance firm that works with credit card companies of a possible security compromise, we conducted an internal review, and then took down our web payments page.
> . . . .
> We hired a third-party external forensics firm to investigate any potential security breach in our systems, migrated our web payments portal services to a third-party vendor, and retained additional experts to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this

---

4 *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory*, DataBreaches.net (May 10, 2019), *available at* https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/.

5 *Id.*

6 *Id.*

> incident. We remain committed to our system's security, data privacy, and the protection of personal information.[7]

### B. CareCentrix's Patient Information Was Exposed By The Data Breach

#### 1. CareCentrix Obtained Personal Information From Plaintiffs And Class Members And Shared That Information With AMCA

36. CareCentrix offers post-acute care to patients by providing programs to "improve quality and lower costs by allowing patients to heal or age where they want to be: at home." CareCentrix provides these home-based services for 26 million members through 8,000 provider locations across the country.[8]

37. Upon information and belief, CareCentrix charges patients for the services it provides to them and its invoices include only fees for such services. Patients are responsible for paying CareCentrix for performing services either through their insurance or out-of-pocket, if the patient does not have insurance or the costs are not entirely covered by insurance.

38. If CareCentrix's patients fail to pay their invoices within the requested time period, CareCentrix employs an associated business for collection. During the relevant time period, based upon information and belief, CareCentrix utilized AMCA as a billing collection agency.

39. Upon information and belief, in order to facilitate collection, CareCentrix provided AMCA with its patients' Personal Information, which AMCA in turn stored in its own computer systems. In addition, as part of AMCA's billing collection services for CareCentrix, Plaintiffs furnished Personal Information directly to AMCA, which AMCA subsequently stored.

---

[7] *LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach, Krebs on Security* (June 4, 2019), https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/; *see also Information about the AMCA Data Security Incident*, LabCorp, https://www.labcorp.com/AMCA-data-security-incident (last updated June 10, 2019).

[8] CareCentrix: About Us, https://www.carecentrix.com/about-us (last accessed Nov. 8, 2019).

### 2. CareCentrix Informs Patients That They Were Impacted By The Data Breach

40. CareCentrix began informing its patients in or around July 2019 that AMCA had been subject to a "data privacy incident" and that the breach may have included their PII and PHI including name, identity of medical providers, and dates of service.

41. CareCentrix also informed its patients that the AMCA breach, which compromised their PII and PHI, occurred between August 1, 2018 and March 30, 2019.

42. On July 11, 2019, CareCentrix advised the OCR of the Data Breach and that 467,621 individuals were impacted. OCR is currently investigating the matter.[9]

43. CareCentrix failed to provide proper, timely notice of the Data Breach sufficient to allow its patients to take steps to protect themselves.

44. Despite the fact AMCA was notified of the data breach on March 20, 2019, CareCentrix did not notify its patients until July 2019.

### 3. CareCentrix Committed To Safeguarding Its Patients' Personal Information

45. CareCentrix agreed that it was bound to the privacy and security policies of the health care plans concerning its patients and that its Privacy Policy supplemented each health care plan policy pursuant to CareCentrix's Customer Agreements with those health care plans.

46. CareCentrix's Privacy Policy—available via its website—applies to all information collected by its website, mobile applications, and online services that operate and link to the Privacy Policy (such as a patient portal, allowing individuals to pay their bills online). CareCentrix's Privacy Policy, like any privacy policy, acknowledges that no website is 100%

[9] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

secure, but that it would at least "take reasonable precautions to safeguard the Personal Information transmitted between visitors and the Services and the Personal Information stored on our servers."[10] In instances where CareCentrix could not guarantee that transmittals of data would be "100% secure," it encouraged users to use its website to communicate, rather than email correspondence, since its website was more secure.[11]

47. CareCentrix thus provided patients with a false sense of security that, by using its website, patients would have a more secure way of providing their PII and PHI to CareCentrix.

48. In a September 27, 2018 press release, CareCentrix touted its data security:

> CareCentrix, a leading provider of post-acute care management, announced that several of their technology platforms used to store, process, maintain, and transmit customer electronic protected health information (ePHI)* have earned Certified status for information security by HITRUST. HITRUST CSF Certified status demonstrates that the CareCentrix technology platforms*, which are used to store, process, maintain, and transmit customer ePHI, have met key regulatory requirements, industry defined requirements, and are appropriately managing risk.[12]

49. CareCentrix further claimed that meeting the above standards placed it in an "elite" group of organizations that have earned this certification which, according to John Driscoll, CareCentrix's Chief Executive Officer, represented the "gold-standard" of security.[13] This

---

[10] CareCentrix Privacy Policy, https://www.carecentrix.com/privacy-policy (last accessed Nov. 9, 2019).

[11] *Id.*

[12] Press Release, CareCentrix Achieves HITTRUST CSF Certification to Manage Risk, Improve Security Posture and Meet Compliance Requirements (Sept. 27, 2018), *available at* https://markets.businessinsider.com/news/stocks/carecentrix-achieves-hitrust-csf-certification-to-manage-risk-improve-security-posture-and-meet-compliance-requirements-1027570669.

[13] *Id.*

certification furthermore demonstrates CareCentrix's commitment to "patient data privacy and safety."[14]

50. These statements were untrue and in stark contrast to the negligent and casual way CareCentrix handed over class members' PII and PHI to AMCA.

51. In addition, HIPAA requires that CareCentrix provide every patient it treats, including Plaintiffs and the putative Class Members, with a privacy notice. In CareCentrix's Notice of Privacy Practices, it states that it uses PII and PHI for limited purposes, including for providing or arranging services, treatment, running its organization, and billing for services.[15]

52. Additionally, CareCentrix vaguely acknowledges that it "will let you know promptly if a breach occurs that may have compromised the privacy or security of your Health Information."[16]

**C. Defendant Failed To Exercise Due Care**

53. Defendant failed to exercise due care in protecting patients' information by contracting with AMCA to handle debt collections.

54. AMCA's bankruptcy filings indicate how thinly capitalized the company was and how insignificant its information technology ("IT") department and infrastructure were. Public reporting has suggested that AMCA is not a reputable business associate—let alone an associate to be trusted with Class Members' Personal Information.

55. Specifically, AMCA's bankruptcy filings admit that it had less than $4 million in liquidity and its owner had to take a secured loan from his own personal money simply to mail

---

14 *Id.*

15 CareCentrix Notice of Privacy Practices, https://www.carecentrix.com/wp-content/uploads/Notice-of-Privacy-Practices-071219-Final.pdf (last accessed Nov. 4, 2019).

16 *Id.*

notices to those impacted by the Data Breach. Put simply, Defendant should not have contracted with an entity that did not even have the means to mail notices to people without having to file for bankruptcy.

56. The length of time between the breach and AMCA's claimed discovery of the breach indicates that AMCA's systems to detect intrusion, detect unusual activity, and log and report such events were woefully inadequate and not in compliance with industry standards. For example, according to technology-security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been on a downward trend in recent years due to improvements in detection computer technology.[17] The fact that it took AMCA 242 days to detect the Data Breach, nearly 3.5 times the median time for detection in 2018, is direct evidence of its failure to employ reasonable, industry-standard data security practices to safeguard Plaintiffs' and Class Members' Personal Information. AMCA's data security deficiencies would have been apparent had CareCentrix adequately investigated.

57. AMCA's inability to detect its own Data Breach, when an unrelated security firm (Gemini Advisory, which was not working for AMCA) was apparently able to do so with ease, is further evidence of the fact that AMCA employed inadequate data-security practices, and that Defendant failed in its independent obligations to ensure that its HIPAA business associate employed reasonable and industry-standard data security measures. The FireEye report indicates

[17] *M-Trends 2019: FireEye Mandiant Services Special Report, available at* https://content.fireeye.com/m-trends (last visited June 11, 2019).

that in 2018, the median amount of time that it took a third-party (like Gemini Advisory) to detect a data breach was three times the median time for internal detection.[18]

58. One of the easiest ways to minimize exposure to a data breach is to limit the type and amount of information provided to third-party business associates and routine destruction or archiving of inactive PII and PHI so that it cannot not be accessed through online channels. Access to millions of patient records through AMCA's online portal should not have been possible, had AMCA maintained appropriate protections. The sheer number of records suggests that AMCA was not destroying or archiving inactive records. Again, Defendant would have discovered this had it exercised adequate oversight over its business associates and audited the data security protocols utilized by AMCA.

59. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). AMCA was not encrypting payment card information according to minimum industry standards of PCI DSS.

60. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive

[18] *Id.*

authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[19]

61. Defendant had an obligation to exercise oversight over AMCA in a manner that would include immediate knowledge of any data security incidents experienced by AMCA that could affect Defendant's patients. For example, AMCA pointed to the fact that it learned of the unauthorized access in March 2019 through a series of CPP notices suggesting that a "disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges." However, Defendant did not learn of the unauthorized access until months later in May 2019.

62. Defendant agreed, and had continuing contractual and common-law duties and obligations, to keep confidential the Personal Information its patients disclosed to it and to protect this information from unauthorized disclosure. Defendant's agreements, duties, and obligations are based on: (1) HIPAA; (2) industry standards; (3) the agreements and promises made to Plaintiffs and Class Members; and (4) Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45. Class Members provided their Personal Information to Defendant with the reasonable belief that Defendant and its business associates would comply with their agreements and any legal requirements to keep that Personal Information confidential and secure from unauthorized disclosure.

63. HIPAA requires that Defendant provide every patient it treats, including Plaintiffs and Class Members, with a privacy notice.

---

[19] *Securing Account Data with the PCI Point –to-Point Encryption Standard v2*, available at https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf (last accessed June 11, 2019).

64. As described herein, Defendant's privacy notices informed Plaintiffs and Class Members that the Defendant would safeguard and protect PII and PHI, and that Defendant could only use or share PHI for specific purposes.

65. As alleged above, AMCA was a "business associate" of Defendant with whom Defendant shared Personal Information of its patients. As Defendant's business associate, AMCA was required to maintain the privacy and security of Plaintiffs' and Class Members' Personal Information. HIPAA mandates that a covered entity (*i.e.*, Defendant) may only disclose PHI to a "business associate" (*i.e.*, AMCA) if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[20] Defendant failed to ensure that its business associate AMCA safeguarded Personal Information of Defendant's patients and that AMCA complied with HIPAA's privacy mandates.

**D. Defendant Violated HIPAA's Requirements To Safeguard Data**

66. Defendant had non-delegable duties to ensure that all information it collected and stored was secure, and that any associated entities with whom it shared member information maintained adequate and commercially-reasonable data security practices to ensure the protection of plan members' Personal Information.

67. Defendant is covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and

[20] *See* 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e).

Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

68. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

69. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

70. HIPAA requires that Defendant implement appropriate safeguards for this information.

71. HIPAA further mandates that covered entities such as Defendant may disclose PHI to a "business associate," such as AMCA, *only* if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[21]

72. HIPAA requires that Defendant provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.* non-encrypted data.

73. Despite these requirements, Defendant failed to comply with its duties under HIPAA and its own Privacy Practices. Indeed, Defendant failed to:

[21] *See* 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e).

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protect Plaintiffs' and the Class Members' Personal Information;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Take safeguards to ensure that Defendant's business associates adequately protect protected health information;

i. Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

74. Defendant failed to comply with its duties under HIPAA and its own privacy policies despite being aware of the risks associated with unauthorized access of members' Personal Information.

### E. Defendant Was On Notice That Highly Valuable Personal Information Of Its Patients Could Be Breached

75. Defendant was, or should have been, aware that it was collecting highly valuable data, for which Defendant knew, or should have known, there is an upward trend in data breaches in recent years.[22] Accordingly, Defendant was on notice of the harms that could ensue if it failed to protect patients' data.

76. HHS' Office for Civil Rights currently lists 550 breaches affecting 500 or more individuals in the past 24 months.[23] CareCentrix has the eleventh-highest number of patients damaged by this Data Breach.[24]

---

22 *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Sept. 27, 2019) ("Our healthcare statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").

23 *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Oct. 9, 2019).

24 *Id.*

77. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[25]

78. The co-founder of Lastline, a network security provider, said that "Hackers target financial companies, like this billing collection company, as they often store sensitive financial information that can be turned into immediate gains."[26]

79. At the end of 2018, the healthcare sector ranked second highest in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[27] With this Data Breach, 2019 has seen the exposure of three times the number of records compromised in 2018.[28]

---

[25] Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Sept. 27, 2019).

[26] Christopher Rowland, *Quest Diagnostics discloses breach of patient records*, WASH. POST, June 3, 2019, https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html?utm_term=.78dd30c03a88 (last visited Sept. 27, 2019).

[27] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center, https://www.idtheftcenter.org/2018-data-breaches (last visited Apr. 21, 2019).

[28] *Healthcare Data Breach Statistics* (August 2019), HIPPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report (last visited Sept. 27, 2019).

80. Other experts have stated that the Data Breach is at "the intersection of three of the types of data that hackers most desire: personal identifying information that can be used for identity fraud, information about medical conditions, and financial account information."[29]

81. This same article has asked: "why did a collections agency have all of this information in the first place?" It also questioned why medical information and Social Security Numbers needed to be provided to debt collectors.[30]

82. Further, Cathy Allen, CEO of Shared Assessments, a cyber-risk management group, stated that "just the types of test proscribed might indicate a type of illness that you would not want employers or insurance companies to have. Thieves often steal and resell insurance data on the internet . . . having other information makes the data more valuable and the price higher."[31]

83. Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers,

---

29 Scott Ikeda, *Third Party Data Breach Hits Quest Diagnostics with 12 Million Confidential Patient Records Exposed*, CPO Magazine, June 11, 2019, https://www.cpomagazine.com/cyber-security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/ (last visited Oct. 7, 2019).

30 *Id.*

31 *Id.*

social security numbers and other Personal Information directly on various dark web[32] sites making the information publicly available.[33]

84. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a Social Security number sells for only $1.[34]

85. Defendant is well aware that its own data and the data it shares with AMCA contains a treasure trove of material for hackers as it has been targeted in the past. In March 2016, CareCentrix experienced a data breach when an unauthorized individual impersonated a CareCentrix employee and obtained W-2 forms and other sensitive information.[35] Defendant was not a stranger to cyberattacks or theft of PII and PHI.

---

[32] The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last accessed June 17, 2019).

[33] *Here's How Much Your Personal Information Is Selling for on the Dark Web,* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 17, 2019); McFarland et al., *The Hidden Data Economy*, at 3, *available at* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited June 17, 2019).

[34] *Study: Few Aware of Medical Identity Theft Risk*, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 10, 2019).

[35] Amy Baxter, Former CareCentrix Employee Continues Fight in Data Breach, Home Health Care News (Apr. 16, 2017), https://homehealthcarenews.com/2017/04/former-carecentrix-employee-continues-fight-in-data-breach/.

### F. Defendant Has Harmed Plaintiffs And Class Members By Allowing Anyone To Access Their Information

86. Defendant caused harm to Plaintiffs and Class Members by sharing their Personal Information with AMCA without properly monitoring a business associate, and AMCA failed to prevent attackers from accessing and stealing this information in the Data Breach.

87. Given the sensitive nature of the Personal Information stolen in the Data Breach—including names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service, and referring doctor) and other personal information (such as credit and debit card numbers, bank account information, insurance, insurance subscriber identification number), hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

88. In fact, many victims of the Data Breach have likely already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

89. The Personal Information exposed in the Data Breach is highly coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web"—and information tied to this Data Breach has already been offered for

sale. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, extortion, and other negative effects.

90. Medical data is particularly valuable to hackers. In June 2016, a hacker reportedly was offering to sell hacked medical records of nearly 700,000 patients for hundreds of thousands of dollars on a "deep web marketplace." [36] Later, the same hacker revealed that he had a database of 9.3 million records from a U.S. insurer that was for sale. [37]

91. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being compromised. HSAs are often tied to specialized debit cards used to make medical-based payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty). Such information is an "easy target" for criminal actors.[38]

---

[36] Healthcare under Attack: What Happens to Stolen Medical Records?, June 30, 2016, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records (last visited Sept. 27, 2019).

[37] Lording it over the healthcare sector: health insurer database with 9.3M entries up for sale, https://www.databreaches.net/lording-it-over-the-healthcare-sector-health-insurer-database-with-9-3m-entries-up-for-sale/, (last visited Sept. 27, 2019).

[38] *Id.*

92. Fraudulent charges have already been linked to Defendant's billing collector's data handling. Another lab impacted by the Data Breach publicly revealed the exposure of patients' Personal Information only after "a disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[39]

93. In addition, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[40] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

94. As explained further by the FTC, medical identity theft can have other serious consequences:

> Medical ID thieves may use your identity to get treatment—even surgery—or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[41]

---

[39] Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 and in Support of "First Day" Motions, *In re Retrieval-Masters Creditors Bureau, Inc.*, No. 19-23185-RDD (Bankr. S.D.N.Y. June 17, 2019), ECF No. 2 at 5-6.

[40] *The Aftermath 2017*, Identity Theft Resource Center, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Aug. 9, 2019).

[41] *Medical ID Theft: Health Information for Older People*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (last visited Oct. 7, 2019).

95. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[42]

96. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. identity theft and fraud resulting from the theft of their Personal Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

[42] *See Study: Medical identity theft is costly for victims,* CNET (Mar. 3, 2010), *available at* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Oct. 11, 2019).

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

h. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

97. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[43]

98. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[44]

---

[43] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Aug. 9, 2019).

[44] U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are*

99. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[45]

100. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendant would have no reason to tout its data security efforts to their actual and potential customers.

101. Consequently, had consumers known the truth about Defendant's data security practices—that it did not adequately protect and store their Personal Information—they would not have entrusted their Personal Information to CareCentrix.

102. Reactions to the Data Breach reflect the severity and breadth of the adverse impact on the American public.

103. The Attorney General of Maryland issued a "Consumer Alert" on June 12, 2019, warning residents that 500,000 CareCentrix patients were affected by the Data Breach. "Massive data breaches like the one experienced by the AMCA are extremely alarming, especially considering the likelihood that personal, financial, and medical information may now be in the

---

*Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007), *available at* http://www.gao.gov/new.items/d07737.pdf.

[45] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Aug. 9, 2019).

hands of thieves and scammers," said Attorney General Frosh. "I strongly urge consumers to take steps to ensure that their information and personal identity is protected."[46]

104. Connecticut Attorney General William Tong, announcing that Illinois and Connecticut's Attorneys General have opened an investigation into the Data Breach, stated:

> The last thing patients should have to worry about is whether their personal information has been compromised by the entities responsible for protecting it. I am committed to ensuring that impacted patients receive timely notification and that the companies involved take precautions to protect consumers' sensitive health and financial information in the future.[47]

105. Other State Attorneys General, including the Attorneys General of Michigan, Minnesota, and North Carolina, have also launched investigations into the Data Breach.[48]

## CLASS ACTION ALLEGATIONS
## NATIONWIDE CLASSES

106. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All natural persons residing in the United States whose Personal Information was compromised in the Data Breach**.**

107. The Nationwide Class asserts claims against Defendant for negligence (Count 1), negligence *per se* (Count 2), unjust enrichment (Count 3), declaratory judgment (Count 4), and breach of implied contract (Count 5). The Class asserts claims against Defendant CareCentrix for

---

[46] Brian E. Frosh, Attorney General, Maryland, Consumer Alert (June 12, 2019), http://www.marylandattorneygeneral.gov/press/2019/061219.pdf.

[47] *Connecticut and Illinois Open Investigation into Quest Diagnostics, LabCorp Data Breach*, The Office of Attorney General William Tong, *available at* https://portal.ct.gov/AG/Press-Releases/2019-Press-Releases/CT-AND-IL-OPEN-INVESTIGATION-INTO-QUEST-AND-LABCORP-DATA-BREACH.

[48] *AMCA Data Breach Tally Passes 20 Million as BioReference Laboratories Added to List of Impacted Entities*, HIPPA Journal, https://www.hipaajournal.com/amca-data-breach-tally-passes-20-million-as-bioreference-laboratories-added-to-list-of-impacted-entities/ (last visited Oct. 9, 2019).

violations of the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110G, *et seq.* (Count 6), and for Breach of Security Regarding Computerized Data, C.G.S.A. §§ 36a-701b, *et seq.* (Count 7). Finally, a Subclass of Florida individuals asserts claims against CareCentrix for violations of the Florida Unfair and Deceptive Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.* (Count 8).

**STATEWIDE SUBCLASSES**

108. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 1 though 4), on behalf of separate statewide subclasses for each (the "Statewide Subclasses"), defined as follows:

> All natural persons residing in that specific state whose Personal Information was compromised in the Data Breach.

109. Excluded from the Nationwide Class and each Statewide Subclass are the Defendant, any entity in which the Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each Statewide Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

110. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, approximately 500,000 CareCentrix patients had their data compromised in the Data Breach. Those individuals' names and addresses are available from Defendant's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved

notice dissemination methods. On information and belief, there are at least thousands of Class Members in each Statewide Subclass, making joinder of all Statewide Subclass members impracticable.

111. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendant had a duty to protect Personal Information;

b. Whether Defendant failed to take reasonable and prudent security measures;

c. Whether Defendant knew or should have known of the susceptibility of AMCA's systems to a data breach;

d. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendant's security measures to protect its systems were reasonable in light known legal requirements;

f. Whether Defendant was negligent in failing to adequately monitor and audit the data security systems of its vendors and business associates;

g. Whether Defendant's efforts (or lack thereof) to ensure the security of patients' Personal Information provided to business associates were reasonable in light of known legal requirements;

h. Whether Defendant's conduct constituted unfair or deceptive trade practices;

i. Whether Defendant violated state law when it failed to implement reasonable security procedures and practices;

j. Which security procedures and notification procedures Defendant should be required to implement;

k. Whether Defendant has a contractual obligation to use reasonable security measures;

l. Whether Defendant has complied with any contractual obligation to use reasonable security measures;

m. What security measures, if any, must be implemented by Defendant to comply with its contractual obligations;

n. Whether Defendant violated state consumer protection and state medical information privacy laws in connection with the actions described herein;

o. Whether Defendant failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the data breach was discovered;

p. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of AMCA's systems and/or the loss of the Personal Information of Plaintiffs and Class Members;

q. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Defendant's failure to reasonably protect their Personal Information; and,

r. Whether Plaintiffs and Class Members are entitled to damages, declaratory relief, or injunctive relief.

112. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal Information was in Defendant's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

113. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

114. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the

court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

115. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendant or would be dispositive of the interests of members of the proposed Class.

116. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the class. The Class and Subclasses consist of individuals who received services from Defendant and whose accounts were placed into collections with AMCA by Defendant. Class Membership can be determined using Defendant's and AMCA's records in their databases.

117. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

118. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendant failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;

c. Whether Defendant failed to adequately monitor and audit the data security systems of their vendors and business associates;

d. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

## CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

### COUNT 1

### NEGLIGENCE
**On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses**

119. Plaintiffs repeat the allegations contained in the preceding paragraphs 1-105 as if fully set forth herein.

120. Plaintiffs bring this claim against Defendant CareCentrix.

121. Defendant required Plaintiffs and Class Members to submit Personal Information to obtain diagnostic and medical services, which Defendant provided to AMCA for billing purposes. Defendant collected and stored the Personal Information for commercial gain.

122. Defendant knew or should have known that AMCA's web payments page was vulnerable to unauthorized access by third parties.

123. Defendant had non-delegable duties to ensure that contractual partners with whom they shared patient information maintained adequate and commercially-reasonable data security practices to ensure the protection of patients' Personal Information.

124. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within its control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

125. Defendant owed a duty of care to Plaintiffs and members of the Class to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

126. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential data as part of the health treatment process. Only Defendant was in a position to ensure that its contractual partners had sufficient safeguards to protect against the harm to Plaintiffs and Class Members that would result from a data breach.

127. Defendant's duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, as well as their own promises regarding privacy and data security to its patients. This duty exists because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they

would be harmed in the future if Defendant did not protect Plaintiffs' and Class Members' information from hackers.

128. Defendant's duties also arose under HIPPA regulations, which, as described above, applied to Defendant and establish national standards for the protection of patient information, including protected health information, which required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The duty also arose under HIPAA's Privacy Rule requirement that Defendant obtain satisfactory assurances from its business associate AMCA that AMCA would appropriately safeguard the protected health information it receives or creates on behalf of the Defendant. 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

129. Defendant's duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

130. Defendant knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its vendors' and business associates' systems, and the importance of adequate security.

131. Defendant breached its common law, statutory, and other duties—and thus were negligent—by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

132. Defendant breached its duties to Plaintiffs and Class Members in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to adequately monitor and audit the data security systems of its vendors and business associates;

d. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of AMCA's network and systems;

f. Failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personal Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

133. Plaintiffs' and Class Members' Personal Information would not have been compromised but for Defendant's wrongful and negligent breach of their duties.

134. Defendant's failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Personal Information of Plaintiffs and Class Members.

135. It was also foreseeable that Defendant's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and other Class Members.

136. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

137. As a direct and proximate cause of Defendant's conduct, Plaintiffs and the Class suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiffs and Class Members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take years to discover and detect; and loss of the value of their privacy and confidentiality of the stolen confidential data, including health data.

## COUNT 2

## NEGLIGENCE PER SE
**On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses**

138. Plaintiffs repeat the allegations contained in the preceding paragraphs 1-105 as if fully set forth herein.

139. Plaintiffs bring this claim against Defendant CareCentrix.

140. Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

141. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires Defendant to obtain satisfactory assurances that their business associates would appropriately safeguard the protected health information it receives or creates on behalf of the Defendant. 45 CFR § 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA. AMCA constitutes a "business associate" within the meaning of HIPAA.

142. HIPAA further requires Defendant to disclose the unauthorized access and theft of the Personal Information to Plaintiffs and the Class Members "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against

adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, 410.

143. Defendant violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' Personal Information, as described herein.

144. Defendant's violations of HIPAA constitute negligence per se.

145. Plaintiffs and Class Members are within the class of persons that HIPAA was intended to protect.

146. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

147. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

148. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

149. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information they obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Defendant, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

150. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

151. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

152. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

153. As a direct and proximate result of Defendant's negligence per se under HIPAA and the FTC Act, Plaintiffs and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

## COUNT 3

## UNJUST ENRICHMENT

**On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses**

154. Plaintiffs repeat the allegations contained in the preceding paragraphs 1-105 as if fully set forth herein.

155. Plaintiffs bring this claim against all Defendant CareCentrix in the alternative to contract-based claims.

156. Plaintiffs and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Defendant and which was ultimately stolen in the Data Breach.

157. Defendant received a monetary benefit from Plaintiffs and Class Members' conferring their Personal Information, which Defendant retains and uses for business purposes and profit.

158. Plaintiffs' and the Class Members' Personal Information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that Personal Information.

159. But for Defendant's commitment to maintain the confidentiality and security of their Personal Information, Plaintiffs and the Class Members would not have provided the information to the Defendant.

160. As a result of the wrongful conduct alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members. Among other things, Defendant continues to benefit and profit from the use of Plaintiffs' and the Class Members' Personal Information, while its value to Plaintiffs and Class Members has been diminished and its exposure has caused Plaintiffs and Class Members harm.

161. Under the doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, from Plaintiffs and Class Members.

162. Equity and good conscience require restitution by the Defendant in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including, specifically, the value to Defendant of the Personal Information that was stolen in the Data Breach and the resulting profits Defendant received and continues to receive from the use of that information.

## COUNT 4

## DECLARATORY JUDGMENT

**On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses**

163. Plaintiffs repeat the allegations contained in the preceding paragraphs 1-105 as if fully set forth herein.

164. Plaintiffs bring this claim against Defendant CareCentrix.

165. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the Personal Information it collected from them. As previously alleged, Defendant owes duties of care to Plaintiffs and Class Members that require them to adequately secure Personal Information.

166. Defendant still possesses Personal Information pertaining to Plaintiffs and Class Members.

167. Defendant has made no announcement or notification that they have remedied the vulnerabilities in its practices and policies regarding ensuring the data security of patients' Personal Information.

168. Accordingly, Defendant has not satisfied its implied contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's lax approaches towards data security has become public, the Personal Information in their possession and in their vendors and business associates' possession is more vulnerable than it was prior to announcement of the Data Breach.

169. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class Members, including the fact that Class Members' Personal Information was available for sale on the dark web.

170. Plaintiffs, therefore, seek a declaration that (a) Defendant's existing data security measures do not comply with its obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Modifying its practices and policies to ensure the business associates to which it provides patients' Personal Information engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering vendors and business associates to promptly correct any problems or issues detected by such third-party security auditors;

b. Modifying its practices and policies to ensure the business associates to which it provides patients' Personal Information engage third-party security auditors and internal personnel to run automated security monitoring;

c. Modifying its practices and policies to ensure the business associates to which it provides patients' Personal Information audit, test, and train security personnel regarding any new or modified procedures;

d. Modifying its practices and policies to ensure the business associates to which it provides patients' Personal Information segment Personal Information by, among other things, creating firewalls and access controls so that if one area of a system is compromised, hackers cannot gain access to other portions of the systems;

e. Modifying its practices and policies to ensure only Personal Information necessary for provision of services is provided to business associates;

f. Modifying its practices and policies to ensure Personal Information not necessary for the provision of services is purged, deleted, and destroyed, and to ensure its business associates likewise purge, delete, and destroy such Personal Information;

g. Conducting regular security checks of the business associates to which it provides patients' Personal Information;

h. Routinely and continually conduct internal training and education to inform internal security personnel how to monitor the data security of business associates to whom patients' Personal Information is provided; and

i. Educating its patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendant's patients must take to protect themselves.

**COUNT 5**
**BREACH OF IMPLIED CONTRACT**
**On Behalf of Plaintiffs and the Nationwide Class against Defendant CareCentrix**

171. Plaintiffs repeat the allegations contained in the preceding paragraphs 1-105 as if fully set forth herein.

172. Plaintiffs and Class Members were required to provide their Personal Information, including names, addresses, Social Security numbers, financial information, and other personal information, to Defendant in order to complete medical and diagnostic tests.

173. When Plaintiffs and Class Members provided their Personal Information to Defendant in exchange for services, they entered into an implied contract with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and adequately notify them if their data had been breached and compromised.

174. Plaintiffs and the Class Members would not have provided and entrusted their Personal Information to Defendant in the absence of the implied contract to keep the information secure.

175. Plaintiffs and the Class Members fully performed their obligations under the implied contract with Defendant by providing their Personal Information, whereas Defendant did not comply with its obligations to keep the information secure.

176. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs and Class Members' Personal Information, which was compromised as a result of the Data Breach.

177. As a direct and proximate result of Defendant's breach of their implied contacts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity as to how their Personal Information is used; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information in their continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

## COUNT 6

## CONNECTICUT UNFAIR TRADE PRACTICES ACT, C.G.S.A. § 42-110G, *et. seq.*
**On Behalf of Plaintiffs and the Nationwide Class against Defendant CareCentrix**

178. Plaintiffs repeat the allegations contained in the preceding paragraphs 1-105 as if fully set forth herein.

179. Plaintiffs bring this claim against all Defendant CareCentrix.

180. Defendant is a "person" as defined by C.G.S.A. § 42-110a(3).

181. Defendant is engaged in "trade" or "commerce" as those terms are defined by C.G.S.A. § 42-110a(4).

182. At the time of filing this Complaint, Plaintiffs have sent notice to the Attorney General and Commissioner of Consumer Protection pursuant to C.G.S.A. § 42-110g(c). Plaintiffs will provide a file-stamped copy of the Complaint to the Attorney General and Commissioner of Consumer Protection.

183. Defendant advertised, offered, or sold services in Connecticut, and engaged in trade or commerce directly or indirectly affecting the people of Connecticut.

184. Defendant engaged in deceptive acts and practices and unfair acts and practices in the conduct of trade or commerce, in violation of the C.G.S.A. § 42-110b, including:

a. Representing that services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

b. Representing that services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

185. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

186. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

187. Had Defendant disclosed to Plaintiffs and Class Members that it misrepresented AMCA's vendor's network security, or otherwise had not omitted to Plaintiffs and Class Members that AMCA's systems were insecure, Defendant would not have been able to continue storing Plaintiffs and Class Members' Personal Information on its network, and would have been forced to disclose the material information regarding AMCA's security. Instead, Defendant failed to discover that AMCA's servers were vulnerable through adequate due diligence and testing, and yet still continued to provide AMCA with Plaintiffs and Class Members' Personal Information.

188. Defendant's unlawful, deceptive, and unconscionable acts include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' Personal Information;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Class Members' Personal Information, including by implementing and

maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' Personal Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Class members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class members' Personal Information.

189. Defendant's conduct was intentional, knowing, and malicious because Defendant knew the value of Personal Information they stored and provided to AMCA and failed to undertake or implement necessary safeguards, controls, and data security measures to keep it secure.

190. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from identity theft, fraudulent charges, loss of value of Personal Information, and time and money spent on preventative and corrective measures.

191. Defendant's deceptive acts and practices caused substantial, ascertainable injury to Plaintiffs and Class members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

192. The application of Connecticut law to the Class is appropriate, given CareCentrix's headquarters in Connecticut; however, discovery will be necessary to address appropriately any choice of law issues.

193. Defendant's violations of Connecticut law were done with reckless indifference to the Plaintiffs and the Class or were with an intentional or wanton violation of those rights.

194. Plaintiffs requests damages in the amount to be determined at trial, including statutory and common law damages, restitution; attorneys' fees, and punitive damages.

## COUNT 7

## BREACH OF SECURITY REGARDING COMPUTERIZED DATA, C.G.S.A. § 36a-701b, *et. seq.*

**On Behalf of Plaintiffs and the Nationwide Class against Defendant CareCentrix**

195. Plaintiffs repeat the allegations contained in the preceding paragraphs 1-105 as if fully set forth herein.

196. Plaintiffs bring this claim against all Defendant CareCentrix.

197. Defendant is a business that conducts business in Connecticut and owns, licenses, and maintains computerized data that includes Personal Information as covered by C.G.S.A. § 36a-701b(b). Defendant also maintains computerized data that includes Personal Information that it does not own as covered by C.G.S.A. § 36a-701b(c).

198. Plaintiffs and Class Members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered by C.G.S.A. § 36a-701b(a).

199. Defendant is required to accurately notify Plaintiffs and Class members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay, not to exceed ninety days after discovery of the breach under C.G.S.A. § 36a-701b(b).

200. Defendant is required to immediately notify Plaintiffs and Class members if it becomes aware of a breach of its data security system which may have compromised personal information it stores but Plaintiffs and Class Members own under C.G.S.A. § 36a-701b(c).

201. Because Defendant was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by C.G.S.A. §§ 36a-701b(b) and (c).

202. By failing to disclose the Data Breach in an accurate and timely manner, Defendant failed to comply with C.G.S.A. §§ 36a-701b(b) and (c). Pursuant to C.G.S.A. § 36a-701b(g), Defendant's failure to comply was an unfair trade practice under the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110a, *et seq*.

203. As a direct and proximate result of Defendant's violations of C.G.S.A. §§ 36a-701b(b) and (c), Plaintiffs and Class members suffered damages, as described above.

204. Defendant's corporate office headquarters and the fact that it centers its operations in Connecticut makes it appropriate to assert this claim on behalf of the Class.

205. Plaintiffs and class members seek relief under C.G.S.A. § 42-110g for the harm they suffered because of Defendant's violations of C.G.S.A. §§ 36a-701b(b) and (c), including actual damages and equitable relief.

**CLAIMS ON BEHALF OF STATE-SPECIFIC SUBCLASSES**

206. In the alternative, the claims asserted above are also brought on behalf of statewide subclasses on behalf of those subclasses and for subclasses with substantially-similar state consumer protection laws.

## COUNT 8

## FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq.*

**On Behalf of Plaintiffs and the Florida Subclass against Defendant CareCentrix**

207. Plaintiffs repeat the allegations contained in the preceding paragraphs 1-105 as if fully set forth herein.

208. Plaintiffs bring this claim on behalf of a Florida Subclass.

209. Plaintiffs bring this cause of action against Defendant CareCentrix ("Defendant," for purposes of this Count).

210. Plaintiffs and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

211. Defendant advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

212. Defendant engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Florida Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass members' Personal Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Florida Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Florida Subclass members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2).

213. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

214. Had Defendant disclosed to Plaintiffs and Subclass Members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Subclass Members' Personal Information as part of the services it provided without advising Plaintiffs and Subclass Members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Subclass Members' Personal Information. Accordingly, Plaintiffs and Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

215. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and practices, Plaintiffs and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

216. Plaintiffs and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

## REQUESTS FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead and Co-Liaison Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiffs and Class and Subclass members compensatory, consequential, and general damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiffs be granted the declaratory relief sought herein;

7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre- and post-judgment interest at the maximum legal rate; and

9. That the Court grant all such other relief as it deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a jury trial on all claims so triable.

CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
*Interim Lead Counsel for Plaintiffs*

By: /s/ James E. Cecchi
JAMES E. CECCHI

Dated: November 15, 2019

Joseph J. DePalma
Bruce D. Greenberg
LITE DEPALMA GREENBERG LLC
570 Broad Street, Suite 1201
Newark, New Jersey 07102
(973) 623-3000

Amy E. Keller
Adam J. Levitt
DICELLO LEVITT GUTZLER LLC
10 North Dearborn Street, 11th Floor
Chicago, Illinois 60602
(312) 214-7900

*Other Labs Track Co-Lead Counsel*

Joseph P. Guglielmo
SCOTT+SCOTT ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Ave, 17th Floor
New York, New York 10169
(212) 223-6444

James Pizzirusso
Katie R. Beran
HAUSFELD LLP
1700 K Street, NW, Suite 650
Washington, DC 20006
(202) 540-7200

Laurence D. King
Mario M. Choi
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
(415) 772-4700

*Other Labs Track Steering Committee*